Enabling Secure Ad-hoc Collaboration

Presenter - Karlo Berket (KBerket@lbl.gov)
Deb Agarwal (DAAgarwal@lbl.gov)
Lawrence Berkeley National Laboratory

Goals

- support collaboration
  - — able to form ad-hoc
  - — add users and services on the fly, as needed
  - — scalable to large established collaborations
- flexible security
  - — includes a range of mechanisms
  - — allows appropriate levels of security
- minimal dependence on any single resource or server
  - — these provide added value when present
- easy to collaborate
  - — no one will use it otherwise

Goals

- support collaboration
  - — able to form ad-hoc
  - — add users and services on the fly, as needed
  - — scalable to large established collaborations
- flexible security
  - — includes a range of mechanisms
  - — allows appropriate levels of security
- **minimal dependence on any single resource or server**
  - — these provide added value when present
- easy to collaborate
  - — no one will use it otherwise

Overview

- what needs to be reevaluated
  - — communication
  - — authentication and authorization
- applications
  - — information-sharing tool (scishare)
  - — Pervasive Collaborative Computing Environment (PCCE) secure messaging tool
- conclusion

Overview

- **secure group communication**
  - — architectures
  - — InterGroup protocols
  - — Secure Group Layer
- information-sharing tool (scishare)
- PCCE secure messaging tool
- conclusion

Secure Group Communication

- (reliably) communicate with the other collaborators
- security
  - — know the identities of the other collaborators
  - — protect information
  - — authorize users
- scalability

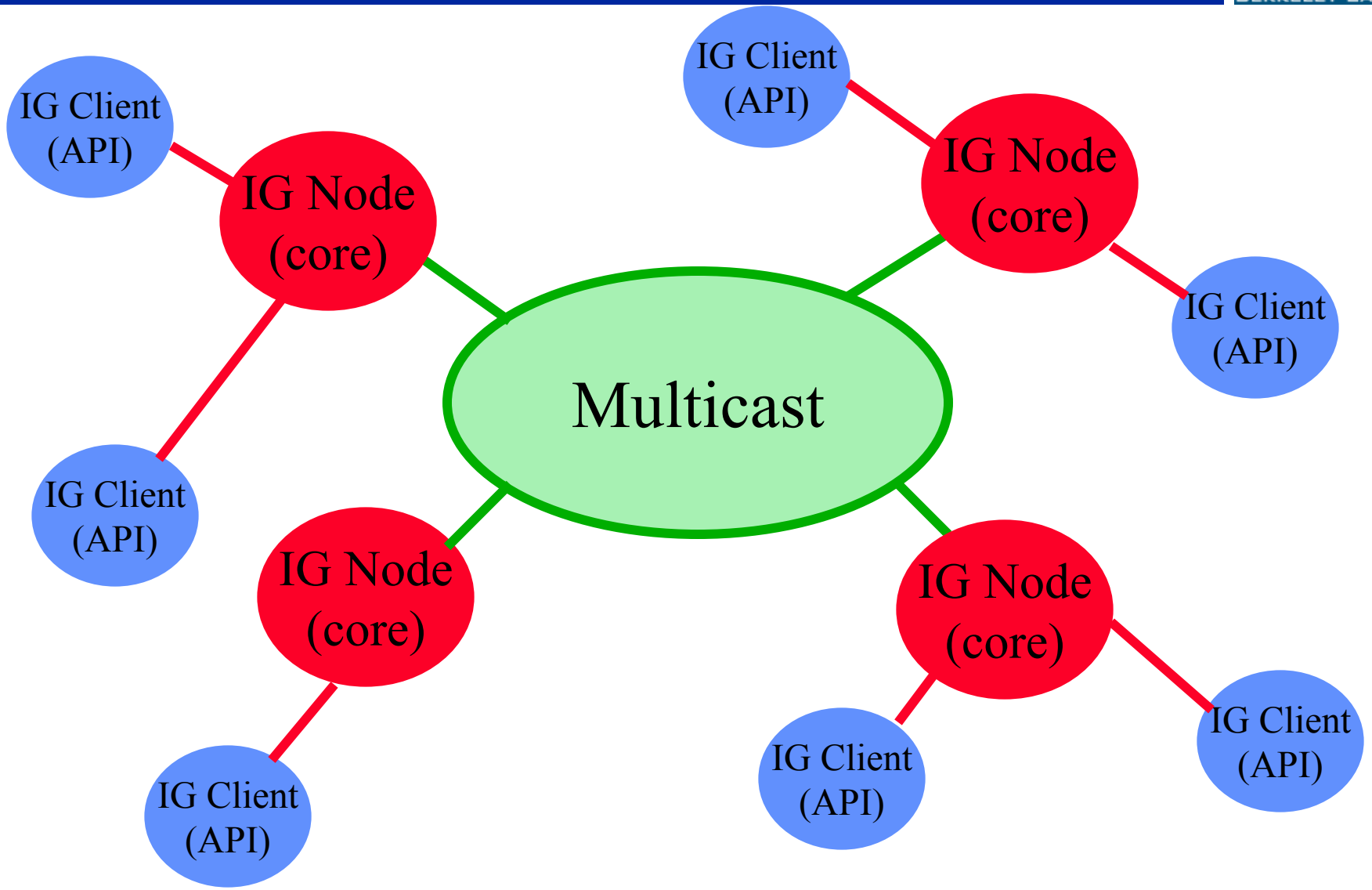
Achieving Secure Group Communication (1)

- unicast mechanisms (TCP and SSL)
  - — architectures
    - centralized server
    - completely connected mesh
    - overlay network
  - — advantages
    - existing infrastructure
    - familiar to developers
  - — disadvantages
    - inefficient
    - single point of failure
    - hard to scale
    - complex to manage

Achieving Secure Group Communication (2)

- IP multicast-based mechanisms (InterGroup and Secure Group Layer)
  - — add to IP multicast
    - acknowledgments and retransmissions
    - membership
    - message ordering
  - — advantages
    - efficient
    - easier to scale
  - — disadvantages
    - lack of IP multicast infrastructure deployment
    - unfamiliar paradigm to developers

InterGroup Architecture



InterGroup Design

- node
  - automatically handles membership, message ordering and retransmission of missed messages
  - uses IP Multicast to transmit messages
- client (API)
  - usable as a library that connects via TCP to the InterGroup node
  - allows machines without multicast connectivity to participate
  - developed for ease of use

Implementation

- current release v1.5
  - — IG Node (Java)
    - deamon listening for client connections
    - flow/congestion control very crude
    - reliable group ordered delivery
  - — IG Client (Java, C++, Python)
    - connects to IG node using TCP
    - C++ client (unix flavors only)
    - Python client is SWIG wrapping of the C++ client

Secure Group Layer Goals

- provide a secure channel for the group
- authorization of group members (individually enforced)
- group key management (not centralized)
- group security optional
- portable implementation

SGL Implementation

- prototype release (in progress) in C++
  - — built using recently proven cryptographic algorithms
  - — targeted for controlled environments
  - — support for anonymous, password-based, and certificate-based modes
  - — uses InterGroup as transport
  - — same API as InterGroup (with security extensions)
    - similar to SSL/TCP model

Overview

- secure group communication
- **information-sharing tool (scishare)**
- PCCE secure messaging tool
- conclusion

Scishare Goals

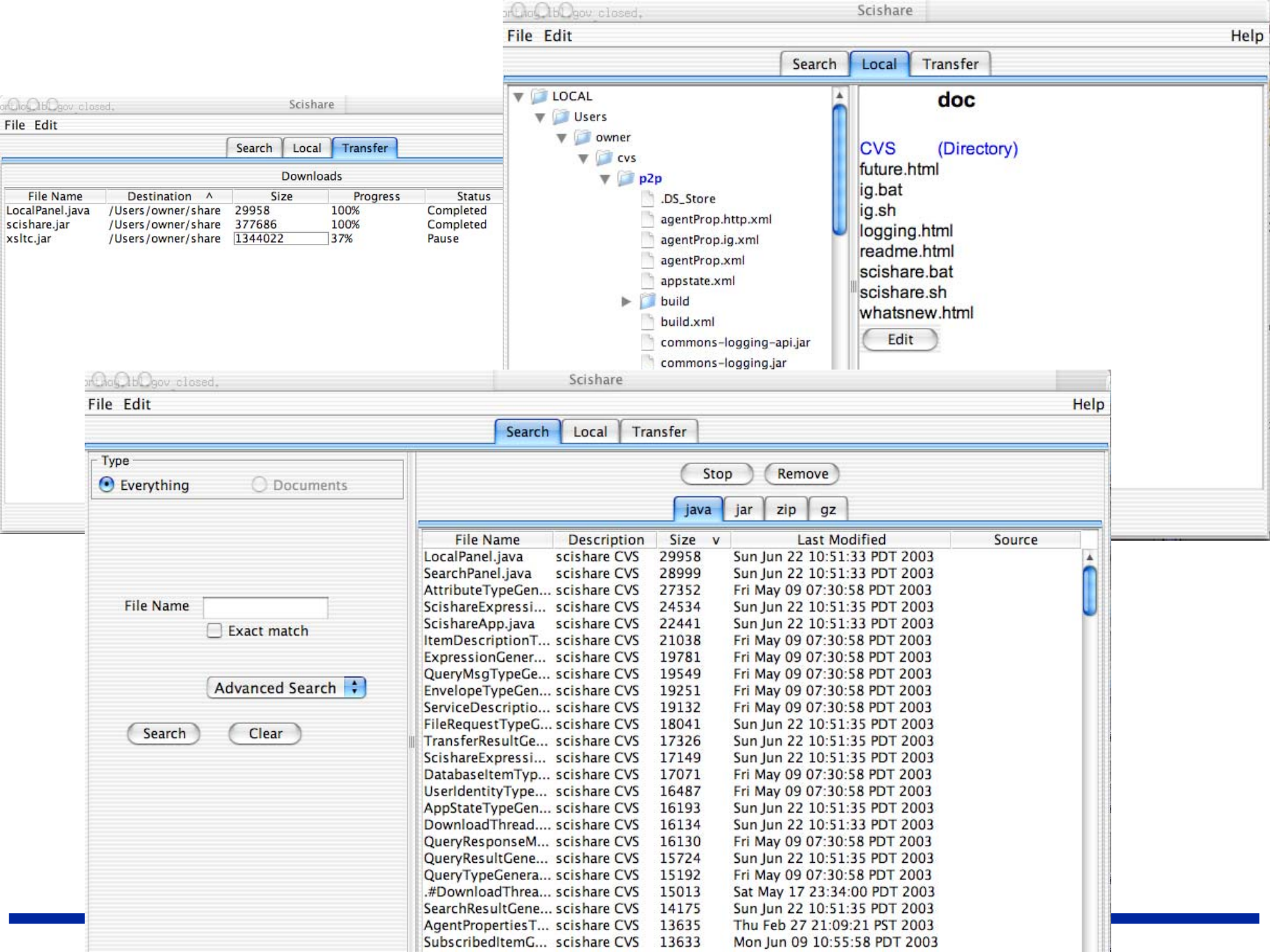
- store and manage information on local storage facilities
- share information with remote participants
- lightweight
- scalable
- secure

What's Different Here?

- use of group communication mechanisms for searching
- security mechanisms and policies for ad hoc information sharing based on
  - — Secure Group Layer (SGL) for securing group communication
  - — support for X.509 identity certificate-based authentication and authorization

Implementation

- initial release scheduled for Q3 2003
- software in Java (requires Java 1.4)
  - — a simple messaging framework for resource discovery (based on XML)
  - — information discovery between hosts using InterGroup and HTTP for communication
  - — search for files by file name, description, and file size
  - — download a file whose metadata was returned as a result of a search
  - — manage sharing of local files


Scishare
File Edit
Help
Search
Local
Transfer
LOCAL
Users
owner
cvs
p2p
.DS_Store
agentProp.http.xml
agentProp.ig.xml
agentProp.xml
appstate.xml
build
build.xml
commons-logging-api.jar
commons-logging.jar
doc
CVS (Directory)
future.html
ig.bat
ig.sh
logging.html
readme.html
scishare.bat
scishare.sh
whatsnew.html
Edit
Downloads
File Name
Destination
Size
Progress
Status
LocalPanel.java
/Users/owner/share
29958
100%
Completed
scishare.jar
/Users/owner/share
377686
100%
Completed
xsltc.jar
/Users/owner/share
1344022
37%
Pause
Type
Everything
Documents
File Name
Exact match
Advanced Search
Search
Clear
Stop
Remove
java
jar
zip
gz
File Name
Description
Size
Last Modified
Source
LocalPanel.java scishare CVS 29958 Sun Jun 22 10:51:33 PDT 2003
SearchPanel.java scishare CVS 28999 Sun Jun 22 10:51:33 PDT 2003
AttributeTypeGen... scishare CVS 27352 Fri May 09 07:30:58 PDT 2003
ScishareExpressi... scishare CVS 24534 Sun Jun 22 10:51:35 PDT 2003
ScishareApp.java scishare CVS 22441 Sun Jun 22 10:51:33 PDT 2003
ItemDescriptionT... scishare CVS 21038 Fri May 09 07:30:58 PDT 2003
ExpressionGener... scishare CVS 19781 Fri May 09 07:30:58 PDT 2003
QueryMsgTypeGe... scishare CVS 19549 Fri May 09 07:30:58 PDT 2003
EnvelopeTypeGen... scishare CVS 19251 Fri May 09 07:30:58 PDT 2003
ServiceDescriptio... scishare CVS 19132 Fri May 09 07:30:58 PDT 2003
FileRequestTypeG... scishare CVS 18041 Sun Jun 22 10:51:35 PDT 2003
TransferResultGe... scishare CVS 17326 Sun Jun 22 10:51:35 PDT 2003
ScishareExpressi... scishare CVS 17149 Sun Jun 22 10:51:35 PDT 2003
DatabaseItemTyp... scishare CVS 17071 Fri May 09 07:30:58 PDT 2003
UserIdentityType... scishare CVS 16487 Fri May 09 07:30:58 PDT 2003
AppStateTypeGen... scishare CVS 16193 Sun Jun 22 10:51:35 PDT 2003
DownloadThread.... scishare CVS 16134 Sun Jun 22 10:51:33 PDT 2003
QueryResponseM... scishare CVS 16130 Fri May 09 07:30:58 PDT 2003
QueryResultGene... scishare CVS 15724 Sun Jun 22 10:51:35 PDT 2003
QueryTypeGenera... scishare CVS 15192 Fri May 09 07:30:58 PDT 2003
.#DownloadThrea... scishare CVS 15013 Sat May 17 23:34:00 PDT 2003
SearchResultGene... scishare CVS 14175 Sun Jun 22 10:51:35 PDT 2003
AgentPropertiesT... scishare CVS 13635 Thu Feb 27 21:09:21 PST 2003
SubscribedItemG... scishare CVS 13633 Mon Jun 09 10:55:58 PDT 2003

Overview

- secure group communication
- information-sharing tool (scishare)
- **Pervasive Collaborative Computing Environment (PCCE) secure messaging tool**
- conclusion

Current PCCE Architecture

- PCCE Server
  - maintains long-lived information (authorized users, available tools, system venues, descriptions, etc.)
  - performs authentication of users (entry point into the system)
- IRC Server
  - back-end for messaging
  - maintains short-lived information (user-created venues, venue participants, etc.)
- PCCE Client
  - user front end
  - communicates with other clients through servers

Future PCCE Architecture

- InterGroup/SGL
  - — used for exchange of short and long lived information
  - — replaces IRC server as back-end for messaging
- PCCE Server
  - — still maintains long-lived information
  - — grants users additional capabilities
- PCCE Client
  - — maintain short-lived information
  - — entry point to the system (limited capabilities without server)

Overview

- secure group communication
- authentication and authorization
- information-sharing tool (scishare)
- Pervasive Collaborative Computing Environment (PCCE) secure messaging tool
- **conclusion**

Conclusion

- InterGroup and SGL provide core communication services for ad-hoc or infrastructure-enabled collaborations
- scishare example of tool designed with this model in mind
- PCCE example of moving from client-server model to ad-hoc model

Authorization and Authentication in Ad Hoc Environments

- central database that most existing systems use may not be available
- shared secrets not feasible in many situations and not scalable
- independent (local) databases difficult to maintain and lead to inconsistencies
- real-time interfaces do not work for unsupervised applications
- likely solution is some combination of the above

More info

- InterGroup protocols
  http://www-itg.lbl.gov/CIF/GroupComm/InterGroup/
- SGL
  http://www-itg.lbl.gov/SecGrpComm/index.html
- scishare
  http://www-itg.lbl.gov/P2P/file-share/
- PCCE
  http://www-itg.lbl.gov/Collaboratories/pcce.html